Amendments to the Claims

Claim 1 (canceled)

Claim 2 (currently amended): The computer program product according to Claim [[1]] 38, wherein [[the]] strong cryptographic techniques are used for the first security association and the second security association and are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claims 3 - 4 (canceled)

Claim 5 (currently amended): The computer program product according to Claim [[1]] 38, wherein the computer-readable program code means for ~~providing secure communications~~ securely sending and the computer-readable program code means for securely receiving further ~~comprises computer-readable program code means for establishing~~ comprise use of a secure channel established between the security enforcement function and the access control function.

Claim 6 (currently amended): The computer program product according to Claim [[1]] 38, wherein the first security association specifies only coarse-grained access control information.

Claim 7 (currently amended): The computer program product according to Claim [[1]] 38, wherein the first authenticated identity associated with the first [[host]] end device is an identification of a user of the first [[host]] end device.

Claim 8 (currently amended): The computer program product according to Claim [[1]] 38, wherein the first authenticated identity associated with the first [[host]] end device is an identification of an application executing on the first [[host]] end device.

Claim 9 (currently amended): The computer program product according to Claim [[1]] 38, wherein the second security association specifies only coarse-grained access control information.

Claim 10 (currently amended): The computer program product according to Claim [[1]] 38, wherein the second authenticated identity associated with the second [[host]] end device is an identification of a user of the second [[host]] end device.

Claim 11 (currently amended): The computer program product according to Claim [[1]] 38, wherein the second authenticated identity associated with the second [[host]] end device is an identification of an application executing on the second [[host]] end device.

Claim 12 (canceled)

Claim 13 (currently amended): The system according to Claim [[12]] 41, wherein [[the]] strong cryptographic techniques are used for the first security association and the second security association and are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claims 14 - 15 (canceled)

Claim 16 (currently amended): The system according to Claim [[12]] 41, ~~wherein the security enforcement function operates in the boundary device, and~~ wherein the means for securely sending and the means for securely receiving ~~providing secure communications~~ further ~~comprises means for establishing~~ comprise use of a secure channel established between the security enforcement function and the access control function.

Claim 17 (currently amended): The system according to Claim [[12]] 41, wherein the security enforcement function also operates in the first [[host]] end device and in the second [[host]] end device, and ~~wherein the means for providing secure communications~~ further comprising: ~~comprises~~

means for ~~establishing secure channels~~ securely communicating between the security enforcement function in the first end device and the access control function to determine whether the first end device can send a particular data packet to the second end device; and

means for securely communicating between the security enforcement function in the [[and]] second [[hosts]] end device and the access control function to determine whether the second end device can receive the particular data packet from the first end device.

Claim 18 (currently amended): The system according to Claim [[12]] 41, wherein the first authenticated identity associated with the first [[host]] end device is an identification of a user of

the first [[host]] end device and/or an application executing on the first [[host]] end device.

Claim 19 (currently amended): The system according to Claim [[12]] 41, wherein the second authenticated identity associated with the second [[host]] end device is an identification of a user of the second [[host]] end device and/or an application executing on the second [[host]] end device.

Claim 20 (canceled)

Claim 21 (currently amended): The method according to Claim [[20]] 44, wherein [[the]] strong cryptographic techniques are used for the first security association and the second security association and are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claims 22 - 23 (canceled)

Claim 24 (currently amended): The method according to Claim [[20]] 44, ~~wherein the security enforcement function operates in the boundary device, and~~ wherein the securely sending step and the securely receiving step ~~of providing secure communications~~ further ~~comprises the step of establishing~~ comprise use of a secure channel established between the security enforcement function and the access control function.

Claim 25 (currently amended): The method according to Claim [[20]] 44, wherein the security enforcement function also operates in the first [[host]] end device and in the second [[host]] end device, and ~~wherein the step of providing secure communications~~ further comprising the steps of:

securely communicating ~~comprises the step of establishing secure channels~~ between the security enforcement function in the first end device and the access control function to determine whether the first end device can send a particular data packet to the second end device; and

securely communicating between the security enforcement function in the [[and]] second [[hosts]] end device and the access control function to determine whether the second end device can receive the particular data packet from the first end device.

Claim 26 (currently amended): The method according to Claim [[20]] 44, wherein the first authenticated identity associated with the first [[host]] end device is an identification of a user of the first [[host]] end device and/or an application executing on the first [[host]] end device.

Claim 27 (currently amended): The method according to Claim [[20]] 44, wherein the second authenticated identity associated with the second [[host]] end device is an identification of a user of the second [[host]] end device and/or an application executing on the second [[host]] end device.

Claim 28 (canceled)

Claim 29 (currently amended): The method according to Claim [[28]] 47, wherein [[the]] strong

cryptographic techniques are used for the first security association and the second security association and are provided by protocols known as Internet Key Exchange and IP (Internet Protocol) Security Protocol.

Claims 30 - 32 (canceled)

Claim 33 (currently amended): The method according to Claim [[28]] 47, wherein:

the step of securely sending and the step of securely receiving ~~providing secure communications between the first security enforcement function and the access control function~~ each further comprise ~~comprises~~ the step of using ~~establishing~~ a first secure channel established between the first security enforcement function and the access control function when the data packet has reached the first boundary device or using ~~; and~~

~~the step of providing secure communications between the second security enforcement function and the access control function further comprises the step of establishing~~ a second secure channel established between the second security enforcement function and the access control function when the data packet has reached the second boundary device.

Claim 34 (currently amended): The method according to Claim [[28]] 47, wherein the first authenticated identity associated with the first [[host]] end device is an identification of a user of the first [[host]] end device and/or an application executing on the first [[host]] end device.

Claim 35 (currently amended): The method according to Claim [[28]] 47, wherein the second

authenticated identity associated with the second [[host]] end device is an identification of a user of the second [[host]] end device and/or an application executing on the second [[host]] end device.

Claim 36 (previously presented): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

establishing a mutually-authenticated connection between a first end device and a second end device using strong cryptographic techniques, wherein the mutually-authenticated connection comprises a first mutually-authenticated network segment between the first end device and a boundary device providing network-layer protection and a second mutually-authenticated network segment between the second end device and the boundary device;

extracting a first authenticated identity associated with the first end device and a second authenticated identity associated with the second end device during the step of establishing the mutually-authenticated connection;

providing secure communications between a security enforcement function operating in the boundary device and an access control function;

providing the extracted first and second authenticated identities, by the security enforcement function, to the access control function;

determining access privileges of the first end device and the second end device, by the access control function, based upon the provided extracted identities;

securely communicating packet-handling directives from the access control function to the security enforcement function, based upon the determined access privileges; and

using the packet-handling directives, by the security enforcement function, to determine whether to forward packets sent by the first end device on the first network segment to the second end device on the second network segment.

Claim 37 (canceled)

Claim 38 (new): A computer program product for providing fine-grained, identity-based access control in a computer networking environment, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for storing, for a security enforcement function operating in a network-layer boundary device, a first authenticated identity associated with a first end device with which the boundary device has established a first mutually-authenticated network-layer security association;

computer-readable program code means for storing, for the security enforcement function, a second authenticated identity associated with a second end device with which the boundary device has established a second mutually-authenticated network-layer security association; and

computer-readable program code means for using the first authenticated identity and the second authenticated identity to determine whether a data packet traveling between the first end device and the second end device over the first security association and the second security association is to be forwarded or discarded upon reaching the boundary device, further comprising:

computer-readable program code means for securely sending the first authenticated identity and the second authenticated identity from the security enforcement function to an access control function, responsive to the data packet reaching the boundary device, such that the access control function can use the securely-sent identities to obtain corresponding access privileges and generate packet-handling directives based thereupon;

computer-readable program code means for securely receiving, by the security enforcement function, the packet-handling directives from the access control function; and

computer-readable program code means, operable at the security enforcement function, for either forwarding or discarding the data packet, depending on the received packet-handling directives.

Claim 39 (new): The computer program product according to Claim 38, wherein the computer-readable program code means for using further comprises computer-readable program code means for examining the data packet to determine the first and second authenticated identities, responsive to the data packet reaching the boundary device and prior to operation of the computer-readable program code means for securely sending.

Claim 40 (new): The computer program product according to Claim 38, wherein the first authenticated identity is obtained for the security enforcement function from the first end device when the boundary device and the first end device establish the first security association and the second authenticated identity is obtained for the security enforcement function from the second end device when the boundary device and the second end device establish the second security

association.

Claim 41 (new): A system for providing fine-grained, identity-based access control in a computer networking environment, comprising:

means for storing, for a security enforcement function operating in a network-layer boundary device, a first authenticated identity associated with a first end device with which the boundary device has established a first mutually-authenticated network-layer security association;

means for storing, for the security enforcement function, a second authenticated identity associated with a second end device with which the boundary device has established a second mutually-authenticated network-layer security association; and

means for using the first authenticated identity and the second authenticated identity to determine whether a data packet traveling between the first end device and the second end device over the first security association and the second security association is to be forwarded or discarded upon reaching the boundary device, further comprising:

means for securely sending the first authenticated identity and the second authenticated identity from the security enforcement function to an access control function, responsive to the data packet reaching the boundary device, such that the access control function can use the securely-sent identities to obtain corresponding access privileges and generate packet-handling directives based thereupon;

means for securely receiving, by the security enforcement function, the packet-handling directives from the access control function; and

means, operable at the security enforcement function, for either forwarding or

discarding the data packet, depending on the received packet-handling directives.

Claim 42 (new): The system according to Claim 41, wherein the means for using further comprises means for examining the data packet to determine the first and second authenticated identities, responsive to the data packet reaching the boundary device and prior to operation of the means for securely sending.

Claim 43 (new): The system according to Claim 41, wherein the first authenticated identity is obtained for the security enforcement function from the first end device when the boundary device and the first end device establish the first security association and the second authenticated identity is obtained for the security enforcement function from the second end device when the boundary device and the second end device establish the second security association.

Claim 44 (new): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

storing, for a security enforcement function operating in a network-layer boundary device, a first authenticated identity associated with a first end device with which the boundary device has established a first mutually-authenticated network-layer security association;

storing, for the security enforcement function, a second authenticated identity associated with a second end device with which the boundary device has established a second mutually-authenticated network-layer security association; and

using the first authenticated identity and the second authenticated identity to determine whether a data packet traveling between the first end device and the second end device over the first security association and the second security association is to be forwarded or discarded upon reaching the boundary device, further comprising steps of:

securely sending the first authenticated identity and the second authenticated identity from the security enforcement function to an access control function, responsive to the data packet reaching the boundary device, such that the access control function can use the securely-sent identities to obtain corresponding access privileges and generate packet-handling directives based thereupon;

securely receiving, by the security enforcement function, the packet-handling directives from the access control function; and

either forwarding or discarding the data packet, at the security enforcement function, depending on the received packet-handling directives.

Claim 45 (new): The method according to Claim 44, wherein the using step further comprises the step of examining the data packet to determine the first and second authenticated identities, responsive to the data packet reaching the boundary device and prior to operation of the securely sending step.

Claim 46 (new): The method according to Claim 44, wherein the first authenticated identity is obtained for the security enforcement function from the first end device when the boundary device and the first end device establish the first security association and the second

authenticated identity is obtained for the security enforcement function from the second end device when the boundary device and the second end device establish the second security association.

Claim 47 (new): A method for providing fine-grained, identity-based access control in a computer networking environment, comprising steps of:

storing, for a first security enforcement function operating in a first network-layer boundary device, a first authenticated identity associated with a first end device with which the first boundary device has established a first mutually-authenticated network-layer security association;

storing, for a second security enforcement function operating in a second network-layer boundary device, a second authenticated identity associated with a second end device with which the second boundary device has established a second mutually-authenticated network-layer security association;

establishing a third mutually-authenticated security association between the first boundary device and the second boundary device; and

using the first authenticated identity and the second authenticated identity to determine whether a data packet traveling between the first end device and the second end device over the first security association, the third security association, and the second security association is to be forwarded or discarded upon reaching either of the boundary devices, further comprising steps of:

securely sending the first authenticated identity and the second authenticated

identity from the first security enforcement function to an access control function, responsive to the data packet reaching the first boundary device, or from the second security enforcement function to the access control function, responsive to the data packet reaching the second boundary device, such that the access control function can use the securely-sent identities to obtain corresponding access privileges and generate packet-handling directives based thereupon;

securely receiving, by the first security enforcement function when the authenticated identities are sent therefrom, or by the second security enforcement function when the authenticated identities are sent therefrom, the packet-handling directives from the access control function; and

either forwarding or discarding the data packet, at the security enforcement function receiving the packet-handling directives, depending on the received packet-handling directives.